International Journal of Smart Sensor and Adhoc Network

Volume 1 | Issue 2 Article 17

2011

Attacks in Wireless Networks

Sachin Dev Kanawat
Department of Computer Engineering, Institute of Technology & Management, Rajasthan, India,
sachinkanawat@gmail.com

Pankaj Singh Parihar
Department of Computer Engineering, Institute of Technology & Management, Rajasthan, India,
pankajsinghparihar2002@gmail.com

Attacks in Wireless Networks

Sachin Dev Kanawat
Department of Computer Engineering,
Institute of Technology & Management,
Rajasthan, India,
e-mail:sachinkanawat@gmail.com

Pankaj Singh Parihar
Department of Computer Engineering,
Institute of Technology & Management,
Rajasthan, India,
e-mail: pankajsinghparihar2002@gmail.com

***Abstract*— Communications in wireless networks has been facilitating numerous emerging applications that require packet delivery from one or more senders to multiple receivers. Communications are susceptible to various kinds of attacks due to insecure wireless channels. Communications in wireless networks remains a challenging and critical issue. This paper presents recent advances in security requirements and services in communications in wireless networks. Wireless networks are being used in many commercial and military applications to collect event driven and real time data. Deployment nature of networks makes them vulnerable to security threats. Due to the resource limitations traditional security measures are not more enough to keep safe the nodes. Research in network security domains has produced several security solutions. In this paper we have observed security mechanisms. We have studied these security mechanisms with respect to packet overheads and compared the packet transmission time, average latency and energy consumption. The comparison shows that the packet overheads are lesser as compared to other schemes. It have been observed that packet delivery ratio decreases when we increase number of nodes while energy and latency increases.**

Keywords- DOS(Denial of serviece), WPAN(Wireless personal area network), WMS(Wireless Mesh Networks)

I. Introduction

Wireless Networks constituting large number of nodes are becoming viable solution to many challenging commercial, domestic, and military applications. Wireless Networks collect and disseminate data from the fields where ordinary networks are unreachable for various environmental and strategic reasons.

Wireless networking has emerged as one of the most promising concept for auto-configurable and self-organizing wireless networking to provide adaptive and flexible wireless connectivity to mobile users. This concept can be used for very different wireless access technologies such as wireless local area network (WLAN), wireless metropolitan area network (WMAN), and wireless personal area network (WPAN) technologies. The work in [2] stated that WMNs are anticipated to resolve the limitations and to significantly improve the performance of ad hoc networks, WLANs, WPANs, and wireless metropolitan area networks.

Due to the computation and power limitations wireless networks are more vulnerable to security threats. Security does not come free, adding heavy security measures in terms of computation power, limitation in memory poses and energy significant challenges in designing a light weight security solution against attacks on wireless networks.

II. Security Requirements

A. Level I Security

It is very first level of security, and is built into any wireless device that can be purchased today. It is based on an algorithm called the Wired Equivalent Privacy (WEP), which is designed to overcome the very most security threats. The WEP encrypts data being transmitted over the network. Only the recipient with the correct WEP address can decrypt the information. It is also used to prevent unauthorized access to wireless networks. However, still here are several outstanding security threats existing within a wireless network environment even within level I security [6]

- **Easy access:** Wireless LANs are enormously easy to find and connect to if the proper security measures are not implemented on the network. Attackers can intrude on the network without needing a physical access to the facility. 'Secure System Identifiers (SSIDs)' are assigned to each wireless network. If the SSIDs are broadcasted over the network, they might be intercepted and hence facilitate unauthorized access.
- **Data Tempering:** Describes the risk that wireless data can be captured and deleted during the course of transmission.
- **Masquerading:** Often occurs when the attacker gains unauthorized access to the wireless networks and imitates an authorized user.
- **Rouge access points:** These are the access points installed within a company without the authorization of the networking system administrator. Access points can be easily installed anywhere. However, depending on the individual installing the access points, proper security measures might not be implemented on the networks, thereby setting up an entry point to hackers and attackers.

To ensure the security of WMNs, the following major security objectives of any application have paramount importance.

• **Confidentiality:** Certain information is only accessible to those who have been authorized to access it. In other words, it ensures that certain information is never disclosed to unauthorized entities. We need to keep them secret from all entities that do not have the privilege to access them, in order to maintain the confidentiality of some classified information,.

Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Exposing such information to enemies could lead to devastating consequences. Routing information must also remain confidential as the information might be valuable for enemies to identify and locate their targets in a battlefield in some cases.

• **Availability:** It ensures the survivability of network services despite denial of service (DoS) attacks. This security requirement is challenged mainly during the DoS attacks, in which all the nodes in the network can be the attack target and hence some selfish nodes make some of the network services unavailable. A DoS attack could be launched at any layer of the network [3]. For instance, on the physical and media access control layers, an adversary could employ jamming signal to interfere with communication on any physical channels.

On the network layer, an adversary could interrupt the routing protocol and may disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target of an adversary is the key management service, which is an essential service for any security framework.

• **Integrity:** Integrity guarantees that a message being transferred will never corrupt. Integrity can be compromised mainly in the following two important ways [9]:

i) Malicious altering - such as an attacker altering an account number in a bank transaction

ii) Accidental altering - such as a transmission error.

A message could be replayed, removed, or revised by an adversary with malicious attack goals on the network, which is regarded as malicious altering. On the contrary, if the message is lost or if its content is changed due to some benign failures, which may be transmission errors in communication such as radio propagation impairment or hardware errors like hard disk failure, then it is categorized as accidental altering.

• **Non-repudiation :** It ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. Non-repudiation is useful for detection and isolation of a node with some abnormal behavior. For instance, when node-A receives an incorrect message from node-B, non-repudiation allows node-A to accuse node-B using this message and to convince other nodes that node-B is compromised.

• **Authenticity :** Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to ensure their identities using some authentication techniques. Without the use of an authentication mechanism, the adversary could impersonate a benign entity and thus gain access to confidential resources.

• **Anonymity: It** means that all the information that can be used to identify the current user or owner should be kept private and not distributed to other communicating parties. This security requirement is very closely related to the preservation of privacy. Hence, we should try to protect the privacy of a user entity from arbitrary disclosure to any other entities.

• **Authorization:** Authorization is a process in which an entity is issued a credential by the trusted certificate authority. It is usually used to assign different access rights to different level of users. For example, we may need to make sure that network management function is only accessible by the network administrator. So, there should be an authorization process before the network administrator accesses the network management functions.

B. Level II Security

This is a mid level security algorithm that addresses most of the security threats not resolved by WEP [4].WPA (Wi-Fi Protected access) applies stronger network access control, also supports better security technologies, and enforces data integrity. WPA however does not respond to all the security threats, and similar to WEP poses some additional concerns and treats:

Encryption weaknesses: WPA has some encryption weaknesses. Therefore, masquerading and data tampering are hot completely resolved by level I security.

Sacrificing performance: Due to intensive computation of encryption protocols and authentication, the system performance degrades, and data transfers and communication speeds are dropped.

C. Level III Security

Finally, the highest level of security available for wireless networks was launched in the early 2004- the 802.1li eliminates most of the security flaws in WEP/WPA level and provides encryption security of 128bit for wireless networks. However, there is deterioration in performance every time a user attempts to perform a transaction, and the network runs scripts to perform security checks and encryption, thus slowing the data transfer rate. Currently, level III is being deployed in specific industries that need the highest level of security to safeguard their information.[4]

III. WMN SECURITY ATTACKS

The main threats that violate the security criteria, which are generally known as security attacks, are analyzed in this section

Impersonation attack: This attack creates a serious security risk in WMNs. If proper authentication of parties is not supported, compromised nodes may be able to join the network, and send false routing information, and masquerade as some other trusted nodes. A compromised node may get access to the network management system of

the network; and it may start changing the configuration of the system as a legitimate user who has special privileges.
Security mechanism of impersonation attacks could be to apply strong authentication methods in contexts where a party has to be able to trust the origin of data it has received or stored.

• **Eavesdropping attack:** An attacker secretly eavesdrops on ongoing communications between targeted nodes to collect information on connection (e.g., medium access control [MAC] address) and cryptography (e.g., session key materials). Although this attack can be classified into other categories such as privacy-related.

• **Denial of service on sensing (DoSS) attack:** An attacker tampers with data before it is read by sensor nodes, thereby resulting in false readings and eventually leading to a wrong decision. A DoSS attack usually targets physical layer applications in an environment where sensor nodes are located.

• **Sybil attacks:** A type of attacks where a node creates multiple illegitimate identities in sensor networks either by stealing or fabricating the identities of legitimate nodes. It can be used against topology maintenance and routing algorithms; it reduces the effectiveness of fault tolerant schemes such as distributed storage and disparity. Another malicious factor is geographic routing where a Sybil node can appear at more than one place simultaneously.

• **Node capture attack:** An attacker physically captures nodes and compromises them such that readings sensed by compromised nodes are manipulated or inaccurate. In addition, the attacker may attempt to extract essential cryptographic keys (e.g., a group key) from wireless nodes that are used to protect communications in the very most wireless networks.

• **Selective forwarding:** In selective forwarding attack, malicious nodes simply drop certain messages instead of forwarding every message. Once a malicious node cherry picks on the messages, it reduces the latency and deceives the neighboring nodes that they are on a shorter route. Effectiveness depends on following two factors. 1) The percentage of messages it drops. 2) Location of the malicious node, the closer it is to the base station the more traffic it will attract. When selective forwarder drops more messages and forwards less, it retains its energy level thus remaining powerful to trick the neighboring nodes.

• **Routing attack:**

Routing attacks in WMNs could be:

Wormhole attack – in this type of attack an attacker receives packets at one location in the network and tunnels them selectively to another location in the network. Then, the packets are resent into the network, and the tunnel between two colluding attackers is referred to as a wormhole.

Routing table overflow attack - an attacker attempts to create routes to nonexistent nodes with intention to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. This attack could also lead to a DoS attack or resource exhaustion.

Byzantine attack - an invalid operation of the network initiated by malicious nodes where the presence of compromised routing and compromised nodes the are not detected. This attack will eventually resulted in sever consequences to the network as the network operation may seem to operate normal to the other nodes.

Sinkhole Black hole/ attack - a malicious node uses the routing protocol to advertise itself as having the shortest path to the node. In this situation, the malicious node advertises itself to a node that it wants to intercept the packet.

Location disclosure attack - this attack reveals something about the locations of nodes or structure of the network such as which other nodes are adjacent to the target, or the physical location of a node.

Hence the routing mechanisms of WMN must be secured. The usual mechanism, to ensure integrity of data, is using hash functions and message digest [2].

IV. Components in Security Requirements

Security never comes for free. When more security features are introduced into the network, in parallel with the enhanced security strength is the ever-increasing communication, computation, and management overhead. Consequently, network performance, in terms of scalability, robustness, service availability, and so on of the security solutions, becomes an important concern in a resource-constrained ad hoc network. While many contemporary proposals focus on the security vigor of their solutions from the cryptographic standpoint, they leave the network performance aspect largely unaddressed. In fact, both dimensions of network performance and security strength are equally important, and achieving a good trade-off between two extremes is one fundamental challenge in security design for wireless network. Figure 1 shows the components of requirements in security for a wireless network.[10]

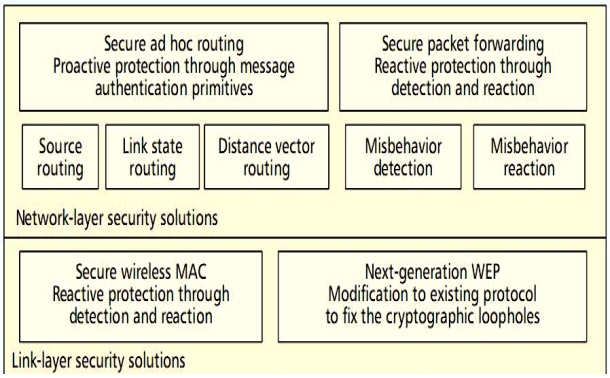

Figure 1. Components in the Security Solution

There are still active research efforts in identifying and defeating more sophisticated and subtle routing attacks. For example, the attacker may further subvert existing nodes in the network, or fabricate its identity and impersonate another legitimate node [1]. A pair of attacker nodes may create a wormhole [5] and shortcut the normal flows between each

other. In the context of on-demand ad hoc routing protocols, the attackers may target the route maintenance process and advertise that an operational link is broken [7].

Layer	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

Figure 2. Security solutions for wireless network should provide complete protection spanning the entire protocol stack

The one fundamental vulnerability comes from their open peer-to-peer architecture. Unlike wired networks that have dedicated routers, each mobile node in a wireless network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in it from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well defined infrastructure where we may deploy even a single security solution.

V. Conclusion

In summary, the major security requirements for the wireless network which should be regarded as a guiding principle to come up with the solutions to the security issues in the Wireless Network are studied and analyzed. The security related features of heterogeneous wireless networks such as sensor networks, WMNs, ad hoc networks, cellular networks WLAN and are briefly discussed. Then we come up with a heterogeneous wireless network integration model that clarifies and integrates the security reference points at the boundaries between heterogeneous networks. Our network integration model provides workable framework for wireless security concerns and for challenges in the realization of open wireless architecture. In addition to this, various security attacks that mainly threaten the Wireless Network are discussed.

References

[1] B. Dahill et al., “A Secure Protocol for Ad Hoc Networks,“ IEEE ICNP, 2002

[2] Ian F. Akyildiz, Xudong Wang and Weilin Wang, “wireless mesh networks: a survey,” Computer Networks, vol. 47, pp. 445-487, Jan. 2005.

[3] X. Gu and R. Hunt, “Wireless LAN Attacks and Vulnerabilities” In the Proceeding of IASTED Networks and Communication Systems, April 2005

[4] Wong S., “The Evolution of Wireless Security in 802. I1 Networks: WEP, WPA and 802.1 I Standards.” SAN Institute May 20,2003. http://vww.sans.orrr/rr/whitepapers/wireless/1109.php, Last accessed December 7,2010.

[5] Y. Hu, A. Perrig, and D. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks,” IEEE INFOCOM, 2002.

[6] Kcng H., “Security Guidelines for Wireless LAN Implementation.” SAN Institure ,August 271h 2003., http://www. Sansorin/lwhitepapcrs/wirelcss/1233.html,LastAccessed: December 6,2010.

[7] Y. Hu, A. Perrig, and D. Johnson, “Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks,“ACM MOBICOM, 2002..

[8] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[9] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity (Accessed on May 24, 2010

[10] D.Liu and P.Neng,“Establishing Pair wise Keys in Distributed Sensor Networks,” Proc. ACM Conf. Computer and Comm. Security (CCS’03),2003.